TREND MICRO™ Securing Your Web World

安全使用社交網絡

趨勢科技香港

內容

- 社交網站的風險
  - 濫用機構網絡
  - 更多風險
  - 攻擊個案分析
- 社交網站用戶應作的準備
  - 如何設定 Facebook以保護私隱

TREND MICRO

社交網站泛濫

TREND MICRO

Source: Brazilian Government

TREND MICRO

工作環境常見活動

1. 查看私人電郵
2. 瀏覽社交網站
3. 使用即時通訊
4. 觀看網上視像
5. 瀏覽與工作無直接關係網站
6. 網上銀行或繳費
7. 網上賭博及遊戲
8. 網上購物
9. 下載執行檔案
10. 作VOIP電話通訊

TREND MICRO

社交網站的風險

- 個人資訊外洩
  - 對社交逐漸失去控制
  - 共享資訊，如圖像或個人資料
    - 通過廣告、下載軟件鏈接、填寫調查盜取資料
    - 免費影片和音樂下載嵌入的木馬程式
- 不當的接觸
  - 網上誘騙
  - 網上欺凌
- 具侵略性或非授意的商業行爲
  - 盜取信息
  - 垃圾電郵
  - 盜取身份
- 在本質上，社交網站活動會令人上癮

TREND MICRO

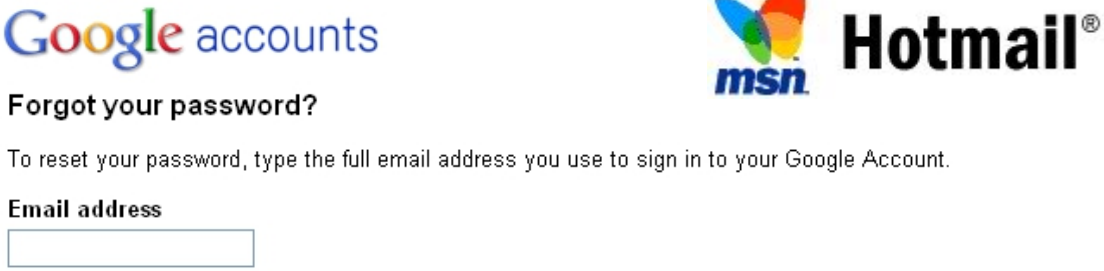
風險來源

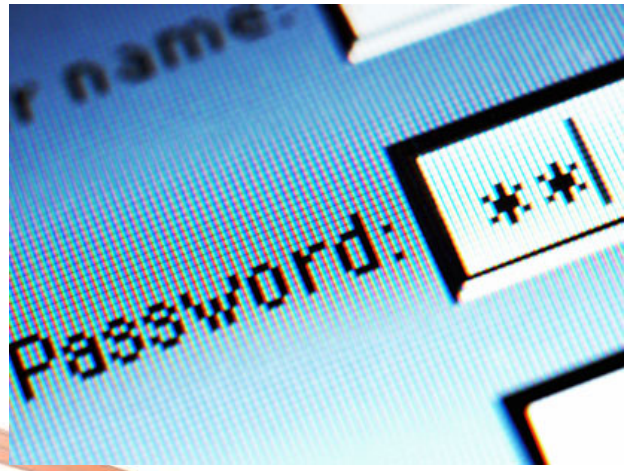
- 虛假戶口
  - 588 虛假 Facebook 戶口
  - 其中179個戶口被Facebook停用
  - 78個戶口成功加入朋友
  - 共成功加入8,278個朋友
  - 平均每個虛假戶口都有 100 個朋友
- 加入朋友
  - 高風險年齡（20-29歲）
  - 高風險國家（美國）

TREND MICRO

個案分析 - Twitter Hack

網上搜尋





http://techcrunch.com/2009/07/19/the-anatomy-of-the-twitter-attack/

TREND MICRO

個案分析 - Twitter Hack

- 後果
  - 3 名Twitter 行政人員的電郵被控制
  - 洩漏財務預算
  - 洩漏員工名單及其信用卡號碼
  - 機密合約
  - 行政人員會議紀錄
    - 夥伴合作計劃
    - 新合約
    - 針對競爭對手的活動

TREND MICRO

個案分析 – KoobFace

- 以社交網站爲目標的殭屍網絡
- 向受感染帳號的好友名單發出僞冒好友訊息，引誘收件人登入Facebook假連結
- 除*Facebook*外，*受影響社交網站包括 MySpace*、*Friendster*、*Twitter*、*hi5*、*NetLog*、 *Tagged* 及 *Bebo*

陷阱

- 連結至假的防毒軟件網站。
- 連結通往加拿大一個背景不明的藥品販賣網站。

TREND MICRO

個案分析 – 美國銀行

- 以殭屍網絡操控電郵戶口，發出含有假網站連結的訊息
- 要求收件人登入連結更新帳戶

陷阱

- 用戶輸入的所有數據都會被盜，後果嚴重。

TREND MICRO

個案分析 – Facebook IQ測驗

- 以殭屍網絡操控電腦，向所有聯絡人發出訊息
- 邀請聯絡人參與IQ測試
- 期間要求輸入手機號碼以接收測試結果

陷阱

- 用戶啓動了「手機內容訂閱」的註冊，訂閱的費用每月從美金**9.99**到**19.99**不等。

TREND MICRO

充分準備 — 一般用戶

- 使用暱稱或代號
- 將個人資料設定私人權限
- 小心守護個人資訊
- 慎思所要張貼的內容
- 保持更新資訊保安軟件
- 領會言外之音
- 避免親自會面
- 己所不欲勿施於人
- 適當對應
- 謹慎使用手機

TREND MICRO

充分準備 — 機構管理層

- 了解保安方案的能力
- 在引進新科技前進行詳細保安評估
- 緊記網絡是無邊際及可流動的
- 訂定公司員工使用社交網絡守則
  - 專責人員負責社交網絡保安，識別危險網站及服務
  - 界定危機及設定目標
  - 訂定策略
  - 充分監察
  - 警醒員工

TREND MICRO

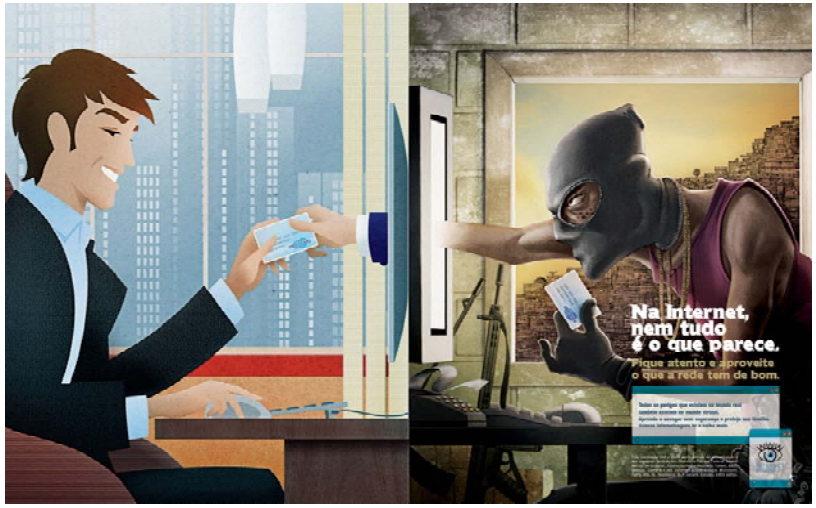
充分準備 — 機構管理層

- 在資訊保安系統定期測試中包含社交工程
- 保持更新資訊保安軟件
- 其他網上行爲可能構成更大危機
  - Webmail（gmail 、 yahoo mail 、 hotmail）
  - 即時通訊（MSN 、 QQ 、 Skype）
  - 端到端及網上分享檔案（BT、Foxy）

TREND MICRO

充分準備 — 一般用戶

- 小心密碼被盜
  - 密碼破解工具：50萬種組合，懶人密碼一一破解
  - 「網路連線出現問題，請重新登錄」：小心是病毒假訊息
  - 間諜軟體
  - 掃描Registry Subkeys：暗中收集密碼，傳送特定 eMail
  - 蠕蟲：電郵和IM 雙管齊下，內建 IM 密碼竊取工具
  - 複製、貼上：網頁惡意程式，專門收集複製貼上的各種密碼
- 小心虛假訊息
  - 惡意連結
  - 殭屍網絡
- 小心守護個人資訊
- 保持更新資訊保安軟件



TREND MICRO

Facebook

- 超過五億用戶
- 超過四億活躍用戶
- 超過3千500萬用戶每日都更新其內容
- 每日超過6千萬條更新
- 每個月上載圖片超過30億幅
- 每週被分享的內容（包括網站連結、新聞、博客、記事及圖片等）超過50億條

建議的 Facebook 保安設定

設定	建議設定
居住城市	一般可以
家鄉	一般可以
愛好及興趣	留空或細想內容會否導致負面評價
尋找對象	留空
政治立場	細想內容會否影響他人對你的觀感及導致網絡欺凌等行爲
宗教觀	一般可以但須細想內容會否影響他人對你的觀感
自我介紹	一般可以但不要過份，須細想別人將如何詮釋你的資料
最喜愛的金句	一般可以，但須定時檢討該金句是否仍是你的心聲
個人資料相片	一幅合適的照片、可代表自己的卡通角色、或干脆留空
感情狀況	留空
教育程度和工作經驗	一般可以列出學校名稱，但建議不要列出僱主
愛好及興趣 （休閒活動、興趣、音樂、書籍、電影、電視）	一般可以，但須細想內容會否影響他人對你的觀感及導致網絡欺凌等行爲

TREND MICRO

建議的 Facebook 保安設定

設定	建議設定
電子郵件	一般可以，但在私隱設定中選擇「僅限朋友」可以看到此資訊
即時通訊的顯示名稱	一般可以，但在私隱設定中選擇「僅限朋友」可以看到此資訊
手機號碼	留空
其他電話號碼	留空
地址	留空
網站	一般可以

TREND MICRO

建議的 Facebook 保安設定

設定	建議設定
基本私隱設定	選擇「僅限朋友」及套用這些設定
近況更新、相片與帖子	僅限朋友
家人	僅限朋友
感情狀態	僅限自己
愛好及興趣	僅限自己
自我介紹和喜愛的佳言絕句	僅限朋友
網站	僅限朋友
宗教觀與政治立場	僅限自己或僅限朋友
曾到訪網站	僅限自己
在我簽到後將我加到「現時在這的人」名單中	不使用

TREND MICRO

建議的 Facebook 保安設定

設定	建議設定
手機號碼	「僅限自己」或僅限自己認識及信任的人
其他電話號碼	「僅限自己」或僅限自己認識及信任的人
地址	僅限自己
即時通訊的顯示名稱	僅限朋友
電子郵件	僅限朋友
你使用的應用程式	定時檢討及移除不恰當的程式
可以透過你的朋友取得的資料	檢討名單，將大部份移除，肯定要關閉「曾到訪網站」
遊戲和應用程式動態	「僅限自己」或自訂至更少人
即時個人化	不要啓用「合作夥伴網站上的即時個人化功能」
公開搜尋	不要啓用

TREND MICRO

建議的 Facebook 保安設定

設定	建議設定	指引
編輯你的黑名單	封鎖令你討厭或希望避開的人	封鎖你希望避開的人，你亦可封鎖來自某些人的應用程式及事件邀請，與及封鎖或解封某些應用系統與你聯繫或使用你的聯絡資料

TREND MICRO

地下經濟活動

TREND MICRO™